ABSTRACT OF THE DISCLOSURE

A method for creating a digital certificate for a user issued by a reliant party, where the reliant party relies on an established cryptographic infrastructure by a registration or certificate authority is described. The registration authority, typically a large financial or credit institution, has already performed the initial overhead steps necessary for a digital authentication system using a chip card. These steps include minting and distributing the chip card, establishing that the key pair and card are given to the right person, and creating the certificate library. The reliant party leverages this cryptographic infrastructure to issue its own digital certificate and certificate chain to a user already having a chip card from the registration authority. Consequently, a user can have additional digital certificates issued to him without having his chip card modified in any way. All additional digital certificates created for a user are stored at a user-specific memory area in a remote certificate library.